FULL CONTENTS

[Claim(s)]

[Claim 1] The main part of information management equipment with which the personal information for two or more persons was stored, and two or more terminal units connected to this main part of information management equipment possible [data communication] through a network, In the personal information management system which reads personal information from said main part of information management equipment through said terminal unit with which it had the portable storage with which this terminal unit is equipped possible [data communication], and was equipped with said portable storage [the personal-data check child generated based on said each personal information / means / to remember that said the personal information on person boils more than one, respectively, and it corresponds / storage] If personal information is required from said main part of information management equipment from said terminal unit The means which reads said personal-data check child remembered by matching with the personal information demanded from said storage means, A collating means to collate the personal-data check child remembered by said portable storage with which this read personal-data check child and said terminal unit were equipped, The personal information management system characterized by providing the management tool which enables the display of said demanded personal information with said terminal unit based on this matching result.

[Claim 2] Said collating means is a personal information management system according to claim 1 characterized by inputting into said portable storage the personal-data check child who read from said storage means, and making him collate inside said portable storage.

[Claim 3] With the personal-data check child who read said management tool from said storage means The personal information management system according to claim 1 or 2 characterized by having a means to read the personal information demanded from said main part of information management equipment, and to transmit to said terminal unit when collating

with the personal-data check child remembered by said portable storage is able to be taken.
[Claim 4] The main part of information management equipment with which the personal information for two or more persons was stored, and two or more terminal units connected to this main part of information management equipment possible [data communication] through a network, In the personal information management system which writes personal information in said main part of information management equipment through said terminal unit with which it had the portable storage with which this terminal unit is equipped possible [data communication], and was equipped with said portable storage A generation means to generate a personal-data check child using the personal information written in at least when writing personal information in said main part of information management equipment, The personal information management system characterized by providing a storage means to match this generated personal-data check child with said personal information, and to remember him, and the means which writes said generated personal-data check child in said portable storage.
[Claim 5] Said generation means is a personal information management system according to claim 4 characterized by generating said personal-data check child by data processing using the characteristic data memorized by the personal information outputted from said terminal unit, and said portable storage in order to write in said main part of information management equipment.
[Claim 6] A means to generate a session key by said main part of information management equipment, to encipher using the public key of said portable storage, and to send out to said portable storage, The personal information management system according to claim 4 characterized by providing a means to encipher said characteristic data with said session key decrypted with said portable storage, and to send out to said main part of information management equipment.
[Claim 7] The personal information management system according to claim 6 characterized by having a means to encipher with the session key generated by said main part of information management equipment, and to send out said said personal-data check child who generated to said portable storage.
[Claim 8] The main part of information management equipment with which the personal information for two or more persons was stored, and two or more terminal units connected to this main part of information management equipment possible [data communication] through a network, Have the portable storage with which this terminal unit is equipped possible [data communication], and said terminal unit with which it was equipped with said portable storage is minded. In the personal information management system which performs read-out and the writing of personal information to said main part of information management equipment [the personal-data check child generated based on said each personal information / means / to

remember that said the personal information on person boils more than one, respectively, and it corresponds / storage] If personal information is required from said main part of information management equipment from said terminal unit The means which reads said personal-data check child remembered by matching with the personal information demanded from said storage means, A collating means to collate the personal-data check child remembered by said portable storage with which this read personal-data check child and said terminal unit were equipped, The management tool which enables the display of said demanded personal information with said terminal unit based on this matching result, and a generation means to generate a personal-data check child using the personal information written in at least when writing personal information in said main part of information management equipment, The personal information management system characterized by providing a check child storage means to match this generated personal-data check child with said personal information, and to remember him, and the means which writes said generated personal-data check child in said portable storage.

[Claim 9] The main part of information management equipment with which the personal information for two or more persons was stored, and two or more terminal units connected to this main part of information management equipment possible [data communication] through a network, In the personal-information-management method which reads personal information from said main part of information management equipment through said terminal unit with which it had the portable storage with which this terminal unit is equipped possible [data communication], and was equipped with said portable storage If personal information is required from said main part of information management equipment from said terminal unit Match with the personal information demanded from said main part of information management equipment, and it memorizes. Read the personal-data check child generated based on said personal information, and it is made to collate with the personal-data check child remembered by said portable storage with which said terminal unit was equipped. The personal-information-management method characterized by enabling the display of said demanded personal information with said terminal unit based on the matching result.

[Claim 10] The personal-information-management method according to claim 9 characterized by making the personal-data check child who read from said main part of information management equipment input into said portable storage, and making him collate inside said portable storage.

[Claim 11] Where collating with the personal-data check child who read from said main part of information management equipment, and the personal-data check child remembered by said portable storage is able to be taken The personal-information-management method according to claim 9 or 10 characterized by reading the personal information demanded from said main part of information management equipment, and transmitting to said terminal unit.

[Claim 12] The main part of information management equipment with which the personal information for two or more persons was stored, and two or more terminal units connected to this main part of information management equipment possible [data communication] through a network, In the personal-information-management method which writes personal information in said main part of information management equipment through said terminal unit with which it had the portable storage with which this terminal unit is equipped possible [data communication], and was equipped with said portable storage When writing personal information in said main part of information management equipment, while matching with the personal information which generated the personal-data check child using the personal information which was outputted from said terminal unit at least, and to write in, and was outputted from said terminal unit and memorizing The personal-information-management method characterized by writing the generated personal-data check child in said portable storage.

[Claim 13] The personal-information-management method according to claim 12 characterized by generating said personal-data check child by data processing using the characteristic data memorized by the personal information outputted to said main part of information management equipment from said terminal unit, and said portable storage.

[Claim 14] Encipher the session key generated by said main part of information management equipment with the public key obtained from said portable storage, and it is made to send out to said portable storage. The personal-information-management method according to claim 12 characterized by enciphering said characteristic data with said session key decrypted with said portable storage, and making it send out to said main part of information management equipment.

[Claim 15] The personal-information-management method according to claim 14 characterized by enciphering with the session key generated by said main part of information management equipment, and sending out said personal-data check child who generated by said main part of information management equipment to said portable storage.

[Claim 16] The main part of information management equipment with which the personal information for two or more persons was stored, and two or more terminal units connected to this main part of information management equipment possible [data communication] through a network, Have the portable storage with which this terminal unit is equipped possible [data communication], and said terminal unit with which it was equipped with said portable storage is minded. In the personal-information-management method of performing read-out and the writing of personal information to said main part of information management equipment If personal information is required from said main part of information management equipment from said terminal unit Match with the personal information demanded from said main part of information management equipment, and it memorizes. Read the personal-data check child

generated based on said personal information, and it is made to collate with the personal-data check child remembered by said portable storage with which said terminal unit was equipped. Based on the matching result, the display of said demanded personal information is enabled with said terminal unit. When writing personal information in said main part of information management equipment, while matching with the personal information which generated the personal-data check child using the personal information which was outputted from said terminal unit at least, and to write in, and was outputted from said terminal unit and memorizing The personal-information-management method characterized by writing the generated personal-data check child in said portable storage.

[Claim 17] The main part of information management equipment with which the chart information for two or more persons was stored, and two or more terminal units connected to this main part of information management equipment possible [data communication] through a network, In the chart information management system which reads chart information from said main part of information management equipment through said terminal unit with which it had the portable storage with which this terminal unit is equipped possible [data communication], and was equipped with said portable storage A storage means to remember the personal-data check child generated based on said each chart information that said more than one correspond to each of the chart information on person, If chart information is required from said main part of information management equipment from said terminal unit The means which reads said personal-data check child remembered by matching with the chart information demanded from said storage means, A collating means to collate the personal-data check child remembered by said portable storage with which this read personal-data check child and said terminal unit were equipped, Chart information management system characterized by providing the management tool which enables the display of said demanded chart information with said terminal unit based on this matching result.

[Claim 18] The main part of information management equipment with which the chart information for two or more persons was stored, and two or more terminal units connected to this main part of information management equipment possible [data communication] through a network, In the chart information management system which writes chart information in said main part of information management equipment through said terminal unit with which it had the portable storage with which this terminal unit is equipped possible [data communication], and was equipped with said portable storage A generation means to generate a personal-data check child using the chart information written in at least when writing chart information in said main part of information management equipment, Chart information management system characterized by providing a storage means to match this generated personal-data check child with said chart information, and to remember him, and the means which writes said generated personal-data check child in said portable storage.

[Claim 19] The main part of information management equipment with which the chart information for two or more persons was stored, and two or more terminal units connected to this main part of information management equipment possible [data communication] through a network, Have the portable storage with which this terminal unit is equipped possible [data communication], and said terminal unit with which it was equipped with said portable storage is minded. In the chart information management system which performs read-out and the writing of chart information to said main part of information management equipment A storage means to remember the personal-data check child generated based on said each chart information that said more than one correspond to each of the chart information on person, If chart information is required from said main part of information management equipment from said terminal unit The means which reads said personal-data check child remembered by matching with the chart information demanded from said storage means, A collating means to collate the personal-data check child remembered by said portable storage with which this read personal-data check child and said terminal unit were equipped, The management tool which enables the display of said demanded chart information with said terminal unit based on this matching result, and a generation means to generate a personal-data check child using the chart information written in at least when writing chart information in said main part of information management equipment, Chart information management system characterized by providing a check child storage means to match this generated personal-data check child with said chart information, and to remember him, and the means which writes said generated personal-data check child in said portable storage.

[Claim 20] The main part of information management equipment with which the chart information for two or more persons was stored, and two or more terminal units connected to this main part of information management equipment possible [data communication] through a network, In the chart information management method which reads chart information from said main part of information management equipment through said terminal unit with which it had the portable storage with which this terminal unit is equipped possible [data communication], and was equipped with said portable storage If chart information is required from said main part of information management equipment from said terminal unit Match with the chart information demanded from said main part of information management equipment, and it memorizes. Said personal-data check child generated based on said chart information is read. The chart information management method characterized by making it collate with the personal-data check child remembered by said portable storage with which said terminal unit was equipped, and enabling the display of said demanded chart information with said terminal unit based on the matching result.

[Claim 21] The main part of information management equipment with which the chart information for two or more persons was stored, and two or more terminal units connected to

this main part of information management equipment possible [data communication] through a network, In the chart information management method which writes chart information in said main part of information management equipment through said terminal unit with which it had the portable storage with which this terminal unit is equipped possible [data communication], and was equipped with said portable storage When writing chart information in said main part of information management equipment, while matching with the chart information which generated the personal-data check child using the chart information which was outputted from said terminal unit at least, and to write in, and was outputted from said terminal unit and memorizing The chart information management method characterized by writing the generated personal-data check child in said portable storage.

[Claim 22] The main part of information management equipment with which the chart information for two or more persons was stored, and two or more terminal units connected to this main part of information management equipment possible [data communication] through a network, Have the portable storage with which this terminal unit is equipped possible [data communication], and said terminal unit with which it was equipped with said portable storage is minded. In the chart information management method of performing read-out and the writing of chart information to said main part of information management equipment If chart information is required from said main part of information management equipment from said terminal unit Match with the chart information demanded from said main part of information management equipment, and it memorizes. Said personal-data check child generated based on said chart information is read. It is made to collate with the personal-data check child remembered by said portable storage with which said terminal unit was equipped. Based on the matching result, the display of said demanded chart information is enabled with said terminal unit. When writing chart information in said main part of information management equipment, while matching with the chart information which generated the personal-data check child using the chart information which was outputted from said terminal unit at least, and to write in, and was outputted from said terminal unit and memorizing The chart information management method characterized by writing the generated personal-data check child in said portable storage.

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to improvement of the personal information management system in the case of sharing personal information, such as chart information, for example, and the personal-information-management method.

[0002]
[Description of the Prior Art] As everyone knows, if it is in a general hospital etc., there is a case where one patient receives medical examination ranging over two or more specialties, plentifully. In this case, that patient's chart information needs to be shared by the doctor of each specialty.
[0003] For this reason, while memorizing patient information on IC (Integrated Circuit) card in the former as indicated, for example to JP,H6-274472,A The terminal unit for performing writing and read-out of data to this IC card is installed in each post, respectively, and the system which enabled it to share patient information between each post through an IC card is developed.
[0004] However, the problem of the storage capacity of the IC card in the present condition being still inadequate, for example, it being unsuitable for memorizing huge chart information, a long-term hospitalization patient's roentgenography or image data by which ultrasonic photography was carried out, etc. by high definition, and causing trouble practically has arisen.

[0005] On the other hand, by recent years, as a management tool of personal information, the client/server system is put in practical use and it considers using a client/server system also for management of chart information.
[0006] By the way, although it has composition which protects data by setting up the access privilege to data in this client/server system There are many points still unsuitable for utilization in respect of security, especially in order to release the chart information to affect a human life on a network and to share it, the room which should improve so that neither alteration nor disclosure can be performed is left behind plentifully.
[0007]
[Problem to be solved by the invention] Then, this invention was made in consideration of the above-mentioned situation, and aims at offering the very good personal information management system and the personal-information-management method of making it possible to share personal information with high security on a network.
[0008]
[Means for solving problem] The main part of information management equipment with which the personal information for two or more persons was stored as for the personal information management system concerning this invention, Two or more terminal units connected to this main part of information management equipment possible [data communication] through a network, It has the portable storage with which this terminal unit is equipped possible [data communication], and is aimed at what reads personal information from the main part of information management equipment through the terminal unit with which it was equipped with the portable storage.

[0009] and [the personal-data check child generated based on each personal information / means / to remember that the personal information for two or more persons is alike, respectively, and it corresponds / storage] The means which reads the personal-data check child remembered by matching with the personal information demanded from the storage means when personal information was required from the main part of information management equipment from the terminal unit, It has a collating means to collate the personal-data check child remembered by the portable storage with which this read personal-data check child and terminal unit were equipped, and the management tool which enables the display of the demanded personal information with a terminal unit based on this matching result.
[0010] [moreover, the personal information management system concerning this invention] The main part of information management equipment with which the personal information for two or more persons was stored, and two or more terminal units connected to this main part of information management equipment possible [data communication] through a network, It has the portable storage with which this terminal unit is equipped possible [data communication], and is aimed at what writes personal information in the main part of information management equipment through the terminal unit with which it was equipped with the portable storage.
[0011] And a generation means to generate a personal-data check child using the personal information written in at least when writing personal information in the main part of information management equipment, It has a storage means to match this generated personal-data check child with personal information, and to remember him, and the means which writes the generated personal-data check child in a portable storage.
[0012] [furthermore, the personal-information-management method concerning this invention] The main part of information management equipment with which the personal information for two or more persons was stored, and two or more terminal units connected to this main part of information management equipment possible [data communication] through a network, It has the portable storage with which this terminal unit is equipped possible [data communication], and is aimed at the method of reading personal information from the main part of information management equipment through the terminal unit with which it was equipped with the portable storage.
[0013] And if personal information is required from the main part of information management equipment from a terminal unit Match with the personal information demanded from the main part of information management equipment, memorize, and the personal-data check child generated based on personal information is read. It is made to collate with the personal-data check child remembered by the portable storage with which the terminal unit was equipped, and is made to enable the display of the demanded personal information with a terminal unit based on the matching result.
[0014] Moreover, the main part of information management equipment with which the personal

information for two or more persons was stored as for the personal-information-management method concerning this invention, Two or more terminal units connected to this main part of information management equipment possible [data communication] through a network, It has the portable storage with which this terminal unit is equipped possible [data communication], and is aimed at the method of writing personal information in the main part of information management equipment through the terminal unit with which it was equipped with the portable storage.

[0015] And when writing personal information in the main part of information management equipment, while matching with the personal information which generated the personal-data check child using the personal information which was outputted from the terminal unit at least, and to write in, and was outputted from the terminal unit and memorizing The generated personal-data check child is written in a portable storage.

[0016] According to the above composition and methods, all can be enabled to share personal information with high security on a network.

[0017]

[Mode for carrying out the invention] The form of implementation of this invention is hereafter explained in detail with reference to Drawings. Drawing 1 shows the outline of the chart information management system explained with the form of this operation.

[0018] [this chart information management system] while two or more hospital terminal 11 and two or more pharmacy terminals 12 which consist of terminal units, such as a personal computer, for example are connected to a network 13, respectively It has the composition that the server 14 which is a main part of information management equipment is connected to this network 13.

[0019] Among these, the hospital terminal 11 is installed, respectively for two or more specialties of every in two or more hospitals of every and the same hospital. Moreover, the pharmacy terminal 12 is installed for two or more pharmacies of every, respectively.

[0020] Furthermore, all the chart information for a majority of every patients is accumulated in the server 14. As this chart information, the information about a patient individual, the information about a medical-examination history, the information about the contents of medical examination, the information about medication, the information about a medical checkup result, the information about the doctor who treated, etc. are included, for example.

[0021] And it is alternatively equipped with patient IC card 15 as a portable information storage medium by which each patient owns the above-mentioned hospital terminal 11 and the pharmacy terminal 12, respectively, and doctor IC card 16 which each doctor owns. And data communication is possible arbitrarily between the hospital terminal 11, the pharmacy terminal 12, the server 14, patient IC card 15, and doctor IC card 16.

[0022] Here, drawing 2 (a) and (b) show the detailed composition of above-mentioned patient

IC card 15. In addition, since above-mentioned doctor IC card 16 is the same composition as patient IC card 15, it omits the explanation.

[0023] Namely, as shown in drawing 2 (a), this patient IC card 15 comes to attach IC18 for signal processing in the card body 17 formed in the size about an abbreviated-name prickle, and can carry them now easily to it.

[0024] [these IC18 for signal processing / the whole / CPU(Central Processing Unit) 19 / and / for controlling in generalization] as shown in drawing 2 (b) ROM (Read) Only Memory20, RAM (Random) It has the composition that Access Memory21, EEP(Electrically Erasable Programmable) ROM22, and the I/O (Input/Output) controller 23 are connected.

[0025] Among these, the control program which CPU19 execute is stored in ROM20. Moreover, RAM21 function as work memory of CPU19 and primary data is stored. Furthermore, I/O controller 23 functions as a control interface for CPU19 to communicate with the hospital terminal 11 or the pharmacy terminal 12 with which it was equipped with this patient IC card 15.

[0026] And in the case of patient IC card 15, details other than personal information, such as a patient's name, a birth date, an address, and the telephone number, are mentioned later, but a password, a patient identifier, a secret key, a personal-data check child, characteristic data, etc. are stored in EEPROM22. Moreover, it is also possible to store the information about medical-examination storage, a medical checkup result, etc. in these EEPROM22.

[0027] In addition, in the case of doctor IC card 16, a password, a doctor identifier, a secret key, etc. other than personal information, such as a doctor's name, an affiliation hospital name, or their affiliation post, are stored in EEPROM22.

[0028] Next, drawing 3 shows the detailed composition of the above-mentioned hospital terminal 11. In addition, since the above-mentioned pharmacy terminal 12 is the same composition as the hospital terminal 11, it omits the explanation.

[0029] [MPU(Micro Processing Unit) 24 / namely, / for this hospital terminal 11 to control the whole in generalization] It has the composition that ROM25, RAM26, the display device 27, a keyboard 28, IC cardI/F(Inter/Face) 29, and the communication device 30 are connected.

[0030] Among these, the control program which MPU24 execute is stored in ROM25. Moreover, RAM26 function as work memory of CPU24 and primary data is stored.

[0031] Furthermore, a liquid crystal display screen etc. is used for the display device 27, for example, and it displays the screen to which the operating state and the predetermined alter operation of the hospital terminal 11 are urged. Moreover, a keyboard 28 functions, in order that a patient or a doctor may perform predetermined alter operation.

[0032] And the above-mentioned IC card I/F29 function as a control interface for MPU24 to communicate with the patient or doctor IC cards 15 and 16 with which this hospital terminal 11 is equipped. Moreover, the communication device 30 functions as a control unit for MPU24 to

communicate with a server 14 through the above-mentioned network 13.

[0033] In the above composition and the made chart information management system, the rough operation is explained with reference to the flow chart shown in drawing 4 . First, when started (Step S11), a doctor makes a doctor's confirming processing perform at Step S12 to the hospital terminal 11 which he wants to use.

[0034] By this confirming processing, if it is checked that using that hospital terminal 11 is the regular doctor permitted, the hospital terminal 11 concerned will permit a doctor's access, and will come to receive a doctor's alter operation.

[0035] Next, a patient makes a patient's confirming processing perform at Step S13 to the hospital terminal 11 which he wants to use. By this confirming processing, if it is checked that using that hospital terminal 11 is the regular patient permitted, the hospital terminal 11 concerned will permit a patient's access, and will come to receive a patient's alter operation.

[0036] Then, a doctor is Step S14, operates the hospital terminal 11 and demands a patient's chart information from a server 14. In this case, the hospital terminal 11 with which the server 14 has required chart information, Predetermined authenticating processing is performed to patient IC card 15 with which this hospital terminal 11 was equipped, and when it has been recognized as it being the just hospital terminal 11 and being just patient IC card 15, the demanded chart information is sent out to the hospital terminal 11.

[0037] Next, a doctor is Step S15, and he performs a medical examination of a patient, looking at the chart information displayed on the display device 27 of the hospital terminal 11. In this case, it is also possible to print chart information.

[0038] And after a medical examination is completed, a doctor is Step S16, operates the hospital terminal 11 and demands the postscript of chart information from a server 14. In this case, although mentioned later for details If the chart information added a postscript is received, while a server 14 will generate a personal-data check child based on that chart information, will make this personal-data check child correspond to all the chart information including a part added a postscript and accumulating it The personal-data check child who generated is seen out to patient IC card 15 via the hospital terminal 11, and it is ended by making the EEPROM22 memorize (Step S17).

[0039] Here, drawing 5 shows in detail processing operation of Step S12 of a flow chart shown in drawing 4 . First, a doctor equips the hospital terminal 11 which he wants to use with doctor IC card 16 which he owns. Then, the hospital terminal 11 requires the input of a password of a doctor on the screen of the display device 27.

[0040] And if a doctor enters a password through a keyboard 28, it will be transmitted to doctor IC card 16 by a verification command from the hospital terminal 11, and the password will be collated within doctor IC card 16. Doctor IC card 16 outputs the status which shows the matching result, and the hospital terminal 11 displays an access permission on a doctor on the

screen of the display device 27, when the status is normal.
[0041] Then, the hospital terminal 11 generates the read command which requires a doctor identifier from doctor IC card 16. Then, doctor IC card 16 outputs a doctor identifier to the hospital terminal 11 based on a read command, the doctor identifier into which the hospital terminal 11 was inputted is memorized, and the confirming processing of the doctor by the hospital terminal 11 is completed here.
[0042] Next, drawing 6 shows in detail processing operation of Step S13 of a flow chart shown in drawing 4 . First, a patient equips the hospital terminal 11 which he wants to use with patient IC card 15 which he owns. Then, the hospital terminal 11 requires the input of a password of a patient on the screen of the display device 27.
[0043] And if a patient enters a password through a keyboard 28, it will be transmitted to patient IC card 15 by a verification command from the hospital terminal 11, and the password will be collated within patient IC card 15. Patient IC card 15 outputs the status which shows the matching result, and the hospital terminal 11 displays an access permission on a patient on the screen of the display device 27, when the status is normal.
[0044] Then, the hospital terminal 11 generates the read command which requires a patient identifier from patient IC card 15. Then, patient IC card 15 outputs a patient identifier to the hospital terminal 11 based on a read command, the patient identifier into which the hospital terminal 11 was inputted is memorized, and the confirming processing of the patient by the hospital terminal 11 is completed here.
[0045] In addition, in this patient confirming processing, the hospital terminal 11 requires the input of a password of a patient. The portion surrounded by the dotted line by drawing 6 does not necessarily need the processing to which access is permitted when the matching result of a password is normal, i.e., to be processed, but depending on the case, it deletes it and you may make it give facilities to a patient.
[0046] Next, drawing 7 shows in detail processing operation of Step S14 of a flow chart shown in drawing 4 . First, the hospital terminal 11 requires a predetermined patient's chart information from a server 14.
[0047] On the occasion of a demand of this chart information, the hospital terminal 11 sends out the terminal identification child whom a patient identifier, a doctor identifier, and hospital terminal 11 the very thing have to a server 14. Thereby, a server 14 is the demand from which hospital terminal 11, and becomes possible [judging which doctor is operating it].
[0048] Moreover, a server 14 memorizes the terminal identification child of a date with access, and the accessed hospital terminal 11, a doctor's accessed doctor identifier, the patient identifier of the patient of whom chart information was required, etc. as a log at this time.
[0049] then, the challenge data X of the random number which the server 14 searched the terminal key K from the terminal identification child, and was itself generated using this

terminal key K -- g'=f (X, K) -- encipherment arithmetic is performed and that result-of-an-operation g' is saved.

[0050] Moreover, a server 14 sends out the generated challenge data X to the hospital terminal 11. the challenge data X supplied from the server 14 in the hospital terminal 11 using the self terminal key K which it has -- g=f (X, K) -- encipherment arithmetic is performed and the result of an operation g is returned to a server 14.

[0051] And [a server 14 collates result-of-an-operation g' of self, and the result of an operation g in the hospital terminal 11, and] if in agreement It judges that it is access from the just hospital terminal 11, and will be in the state of permitting access from this hospital terminal 11, and the authenticating processing of the hospital terminal 11 by a server 14 will be completed here.

[0052] Then, a server 14 is sent out to patient IC card 15 equipped with the personal-data check child remembered with the demanded chart information via the hospital terminal 11 there.

[0053] With then, the personal-data check child to whom the CPU19 were supplied from the server 14 in patient IC card 15 The personal-data check child stored in EEPROM22 of self is collated, and the authenticating processing of patient IC card 15 according to a server 14 here according to return sushi to a server 14 is completed via the hospital terminal 11 in the matching result.

[0054] And a server 14 sends out the demanded chart information to the hospital terminal 11, when the matching results returned from patient IC card 15 are the contents of the purport that both the personal-data check child is in agreement. Thereby, the doctor can see the demanded chart information now with the display device 27 of the hospital terminal 11.

[0055] In this case, the authenticating processing of patient IC card 15 by a server 14 is faced. Are trying to compare the personal-data check child whom the server 14 saw out inside patient IC card 15. That is, since he is trying not to output the personal-data check child stored in EEPROM22 of patient IC card 15 to the exterior of patient IC card 15, security can be raised.

[0056] Thus, after performing a medical examination of a patient and completing a medical examination, looking at the chart information which the doctor demanded, by drawing 4 , as shown in Step S16, a doctor newly creates the chart information added a postscript on the hospital terminal 11, and the postscript of chart information is required from a server 14. Thereby, the chart information added a postscript is sent out and accumulated in a server 14.

[0057] In this case, a doctor makes a server 14 memorize one's electronic signature with the chart information to add. It becomes possible to clarify by this which doctor examined.

[0058] At this time, a secret key peculiar to a doctor is stored in doctor IC card 16, and the signature which can be created only with this secret key is attached to the chart information added a postscript. A public key cryptosystem is used as a method of creating this electronic

signature.

[0059] Moreover, a doctor inputs prescription information into the hospital terminal 11. Then, the hospital terminal 11 operates so that the prescription information may be written in a server 14 and patient IC card 15.

[0060] Here, a server 14 will generate a new personal-data check child based on the electronic signature of the chart information, prescription information, and a doctor, etc. and the characteristic data memorized by patient IC card 15, if the chart information added a postscript is received.

[0061] And while this newly generated personal-data check child makes it correspond to all the chart information including a part added a postscript and being accumulated in a server 14, it is sent out to patient IC card 15 via the hospital terminal 11, and is rewritten with the personal-data check child remembered by those EEPROM22.

[0062] Drawing 8 shows creation processing operation of such a personal-data check child in detail. First, a server 14 searches a patient's public key L from a database based on the patient identifier supplied from patient IC card 15.

[0063] and session key Y which uses a server 14 only in this session using this public key L -- h=f (Y, L) -- encipherment arithmetic is performed, encryption processing is performed and that enciphered session key h is sent out to patient IC card 15 via the hospital terminal 11.

[0064] Then, patient IC card 15 takes out session key Y by decrypting encryption session key h supplied from the server 14 using a secret key. The characteristic data stored in EEPROM22 by this taken-out session key Y are enciphered, and it sends out to a server 14 via the hospital terminal 11.

[0065] By decrypting the encryption characteristic data supplied from patient IC card 15 using session key Y, a server 14 takes out a patient's characteristic data and These characteristic data, A new personal-data check child is generated based on the electronic signature of the above-mentioned chart information added a postscript, prescription information, and a doctor etc.

[0066] As shown in drawing 9 , this personal-data check child's generation inputs the electronic signature of the chart information added a postscript, prescription information, and a doctor, etc. and a patient's characteristic data into the hash-function operation part 31 which was prepared in the server 14 and which is a tropism function on the other hand, and is performed by performing a hash-function operation.

[0067] And the personal-data check child created in this way is seen out to patient IC card 15 via the hospital terminal 11, after encryption processing is performed using session key Y, while being accumulated in the server 14.

[0068] Then, in patient IC card 15, the personal-data check child who received will be decrypted using session key Y, it will write in EEPROM22, and a new personal-data check

child's generation processing and the storage to the server 14 and patient IC card 15 will be performed here.

[0069] And it becomes the signal of the end of access to the server 14 to one chart information that the new personal-data check child was seen out to patient IC card 15 from this server 14.

[0070] When the chart information accumulated in the server 14 is altered here The personal-data check child remembered by patient IC card 15 and the personal-data check child added to the chart information accumulated in the server 14 become things, and it becomes possible to discover that chart information was altered. Moreover, since the characteristic data (secret key) which exist only in patient IC card 15 are used for a personal-data check child's generation, a third party is unable to create.

[0071] Thus, the patient whom the medical examination ended has his patient IC card 15, goes to a pharmacy, and equips said pharmacy terminal 12 with the patient IC card 15. Then, the pharmacy terminal 12 reads a patient identifier from patient IC card 15, adds the terminal identification child of self, and requires chart information of a server 14.

[0072] In this case, after a server 14 performs authenticating processing which was previously explained by drawing 7 to the pharmacy terminal 12 and patient IC card 15, Since it can recognize that it is access from the pharmacy terminal 12 based on the supplied terminal identification child, only for example, required prescription information is transmitted to the pharmacy terminal 12 in a pharmacy. It enables this to prevent the unnecessary outflow of personal information.

[0073] In addition, it is possible to read the prescription information memorized by patient IC card 15 by a card reader, and to prepare medicine in the pharmacy which does not have an accessible terminal in a server 14.

[0074] Next, drawing 10 shows the modification of the above-mentioned form of operation. If this attaches and explains the same sign to the same portion as drawing 1 , the telephone 32 of a patient's house will be connected to a network 13, and a patient will enable it to reserve a hospital using telephone 32.

[0075] First, a patient accesses a server 14 through the telephone 32 of a house, and inputs the patient identifier of self by the key stroke of telephone 32 according to the voice guidance from a server 14. Then, a server 14 retrieves the patient's chart information based on the inputted patient identifier.

[0076] Next, a patient inputs the information set containing time to reserve as the hospital to which he wants to go etc. by the key stroke of telephone 32 according to the voice guidance from a server 14. Then, a server 14 will be kept to the primary buffer which can transmit the reservation patient's chart information to the hospital which reserved, if an information set is notified to the hospital terminal 11 of the specified hospital and reservation is permitted. This becomes possible to correspond promptly to a demand of the reserved chart information from

a hospital.

[0077] Thus, also when transmitting a patient to other hospitals from a hospital, for example by sharing chart information between two or more hospital and two or more pharmacies, chart information can be quickly transmitted to the hospital of the destination.

[0078] In addition, this invention is not limited to the above-mentioned form of operation, in the range which does not deviate from that summary in this outside, can deform variously and can be carried out.

[0079]

[Effect of the Invention] As explained in full detail above, according to this invention, the very good personal information management system and the personal-information-management method of making it possible to share personal information with high security on a network can be offered.

[Brief Description of the Drawings]

[Drawing 1] The figure shown in order to explain the form of implementation of this invention.

[Drawing 2] The figure shown in order to explain the details of the patient IC card in the form of this operation.

[Drawing 3] The figure shown in order to explain the details of the hospital terminal in the form of this operation.

[Drawing 4] The flow chart shown in order to explain rough operation in the form of this operation.

[Drawing 5] The figure shown in order to explain the details of doctor confirming processing operation of the hospital terminal in the form of this operation.

[Drawing 6] The figure shown in order to explain the details of patient confirming processing operation of the hospital terminal in the form of this operation.

[Drawing 7] The figure shown in order to explain the details of processing operation of the demand of the chart information in the form of this operation.

[Drawing 8] The figure shown in order to explain the details of creation processing operation of a personal-data check child in the form of this operation.

[Drawing 9] The figure shown in order to explain the example of data processing which creates the personal-data check child in the form of this operation.

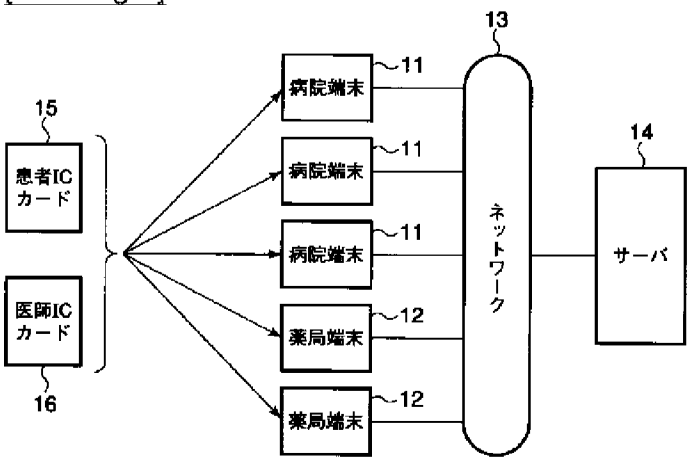
[Drawing 10] The figure shown in order to explain the modification in the form of this operation.

[Explanations of letters or numerals]

11 -- Hospital terminal,

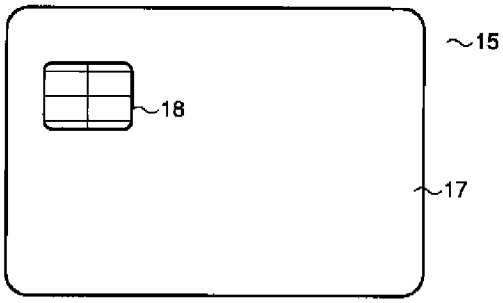
12 -- Pharmacy terminal,
13 -- Network,
14 -- Server,
15 -- Patient IC card,
16 -- Doctor IC card,
17 -- Card body
18 -- IC for signal processing,
19 -- CPU,
20 -- ROM,
21 -- RAM,
22 -- EEPROM,
23 -- I/O controller
24 -- MPU,
25 -- ROM,
26 -- RAM,
27 -- Display device,
28 -- Keyboard,
29 -- IC card I/F,
30 -- Communication device,
31 -- Hash-function operation part,
32 -- Telephone.

[Drawing 1]

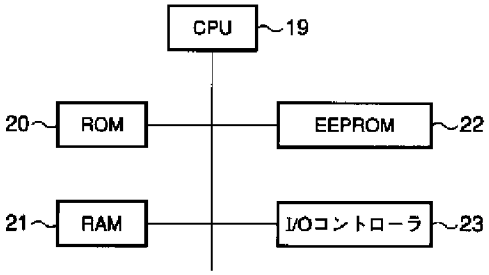


[Drawing 2]

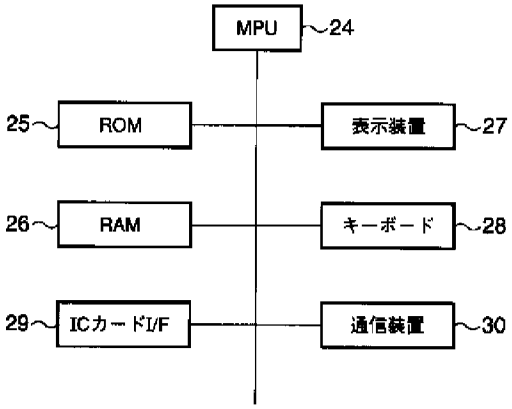
(a)



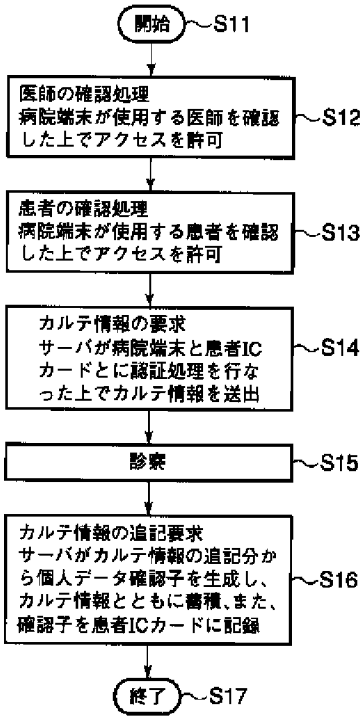
(b)



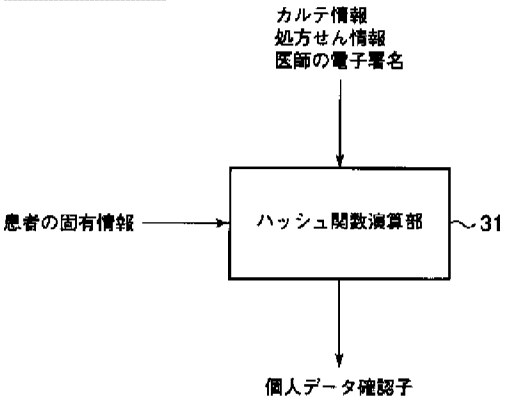
[Drawing 3]



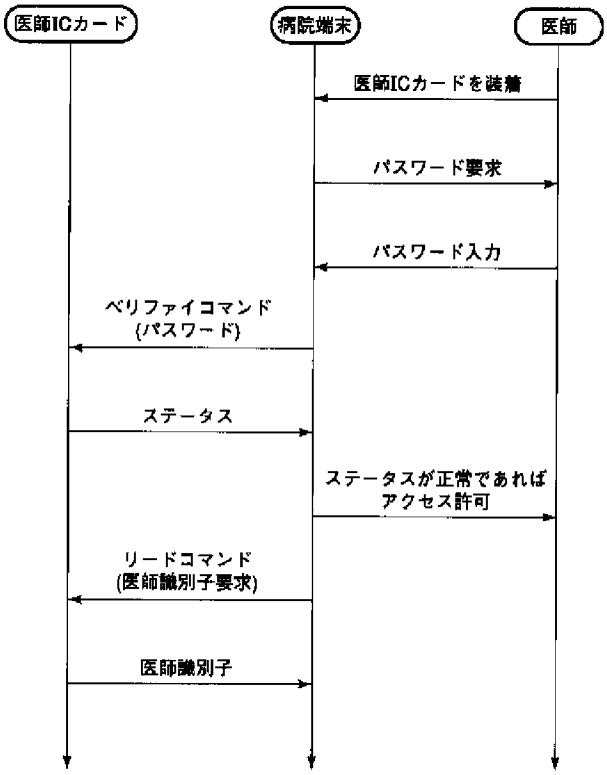
[Drawing 4]



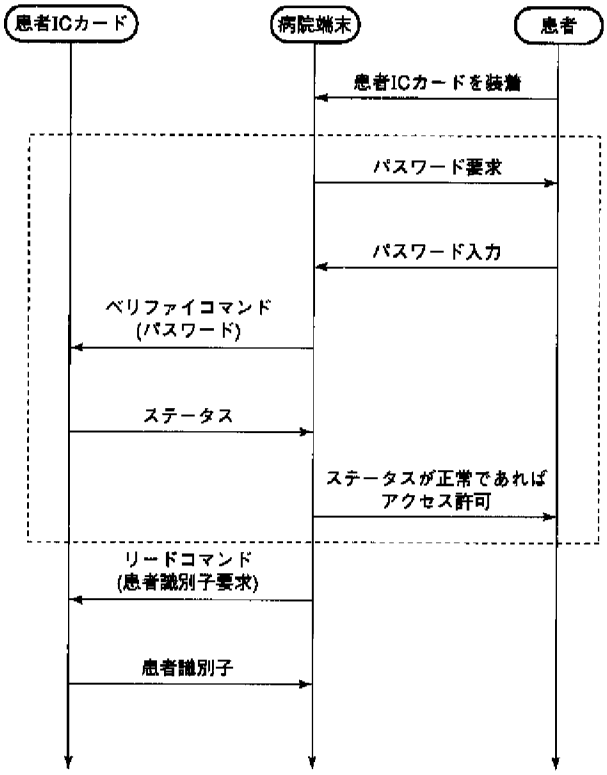
[Drawing 9]



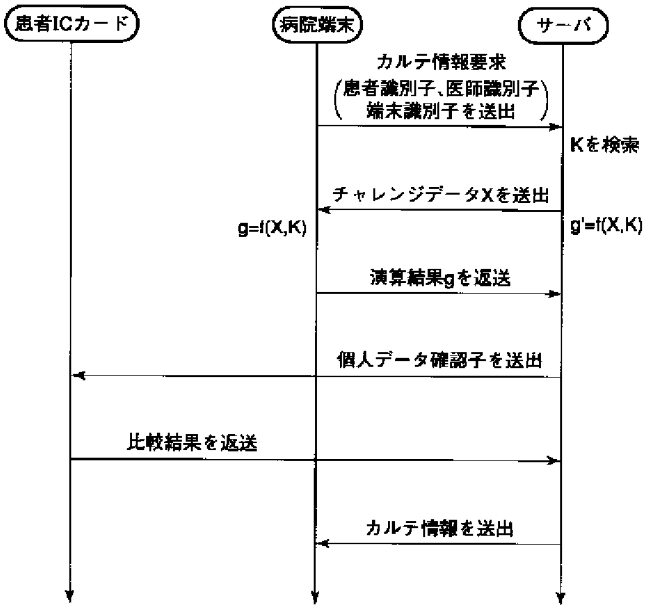
[Drawing 5]



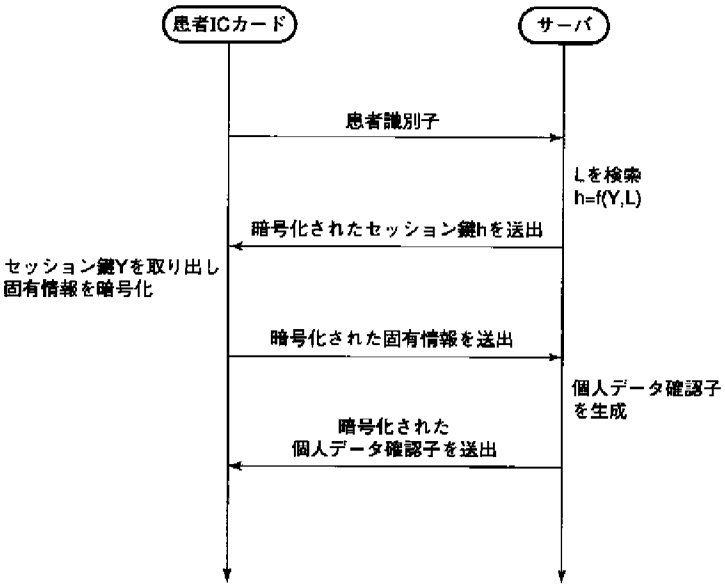
[Drawing 6]



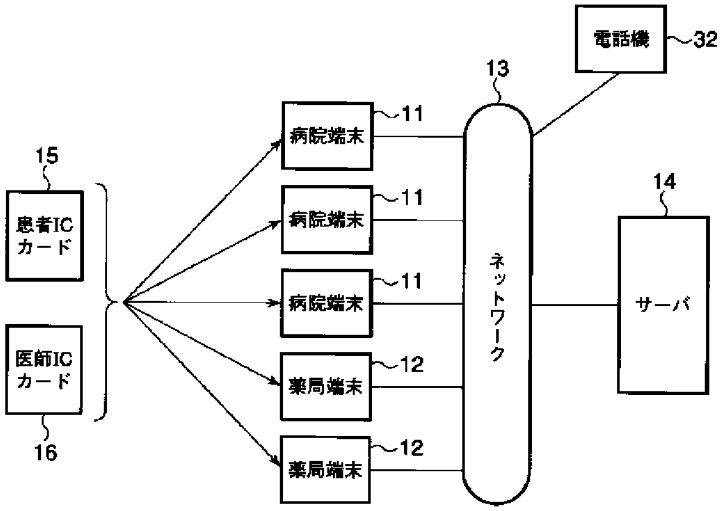
[Drawing 7]



[Drawing 8]



[Drawing 10]



[Translation done.]